Amendments to the claims:

1. (currently amended) Method of updating an authentication algorithm ~~in at least one~~ used by a device (CARD) to authenticate with a data processing device (~~CARD,~~ SERV) ~~which~~ wherein the device (CARD) can store in a memory element of said device (CARD~~, SERV~~) a subscriber identity (IMSI1) which is associated with a first authentication algorithm (Algo1), comprising:

- a preliminary step of storing a second inactive authentication algorithm (Algo2) in a memory element of the device (CARD); and
- a step for switching from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2) including inhibiting the first authentication algorithm (Algo1) and activate the second authentication algorithm (Algo2) used by the device (CARD).

2. (Previously Presented) Method according to claim 1, wherein the switching step is carried out on the initiative of an entity (OP) external to said device.

3. (Previously Presented) Method according to claim 1 or 2, wherein, to perform the switching operation, the entity (OP) external to said device transmits a command (COM) remotely to said device (CARD) in order to switch from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2).

4. (Previously Presented) Method according to claim 1 or 2, wherein, to perform the switching operation, the entity external to said device downloads into the device a program which can start up after a time delay and whose purpose is to switch from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2).

5. (Currently Amended) Method according to claim 1, wherein, during the pre-storage step, a second code IMS12, different from a code IMSI1 associated with the

first algorithm, and associated with the algorithm AIgo2, is stored, and wherein after the step for switching accounts on said device (CARD), said device (CARD) transmits the code IMS12 to all or some of the data processing devices (SERV) whose algorithms need to be switched, said second code (IMSI2) associated with the second algorithm informing these data processing devices that the algorithms have been switched in order to synchronise the algorithm update.

6. (Previously Presented) Method according to claim 5, wherein on reception of the second code (IMSI2) associated with the second authentication algorithm (Algo2), said receiving device switches algorithm from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2).

7. (Previously Presented) Method according to claim 1, wherein after switching, the memory space storing the data associated with the deactivated account is reused.

8. (Previously Presented) Data processing device, in particular a smart card which can store a subscriber identity (IMSI1) and which is associated with a first authentication algorithm (Algo1), comprising:

- memory means storing a second authentication algorithm (Algo2),
- a microcontroller programmed to carry out a step for switching from the first authentication algorithm (Algo1) to the second authentication algorithm (Algo2), which can inhibit the first authentication algorithm (Algo1) and activate the second authentication algorithm (Algo2).

9. (Cancelled)

10. (Cancelled)

11. (Currently Amended) A computer storage media operable to store instructions for instructing a data processing device, in particular a smart card, to perform certain operations, the storage media comprising:

a second inactive authentication algorithm (Algo2)); and

instructions to direct the data processing device(CARD) to execute a step for switching from a first authentication algorithm (Algo1) to a second authentication algorithm (Algo2), which can inhibit the first authentication algorithm (Algo1) and activate the second authentication algorithm.

12. (Currently Amended) The storage media according to claim 11, further comprising instructions to direct the data processing device to~~, after~~ perform the step of switching from the first authentication algorithm to the second authentication algorithm, upon receiving from a transmitting device a code IMSI2 ~~identify the algorithm used by a transmitting device with the code IMSI2,~~ different from the code IMSI1 and therefore associated with the second authentication algorithm Algo2~~, received from said transmitting device when the authentication algorithm is executed on the data processing device~~.